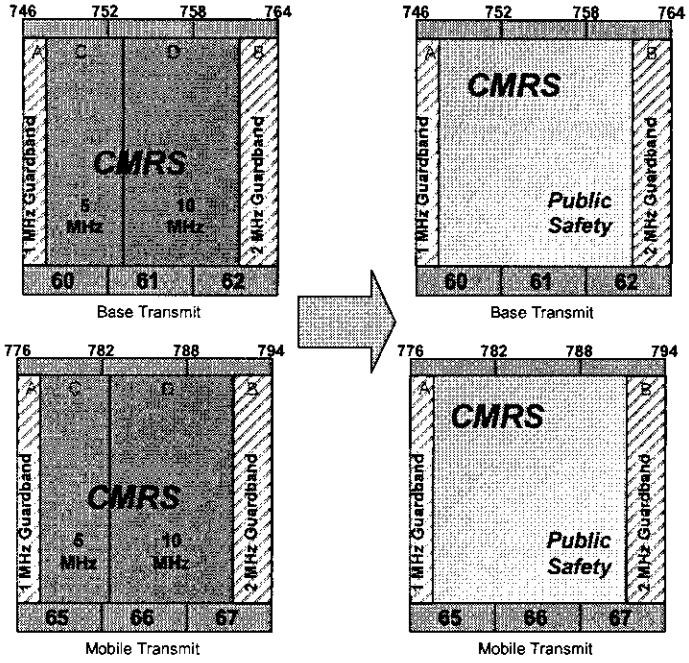

Figure 8 – Creating a Public/Private partnership

Phase 2 – Allow Compatible Broadband Technology in the lower Public Safety band (764 MHz +)

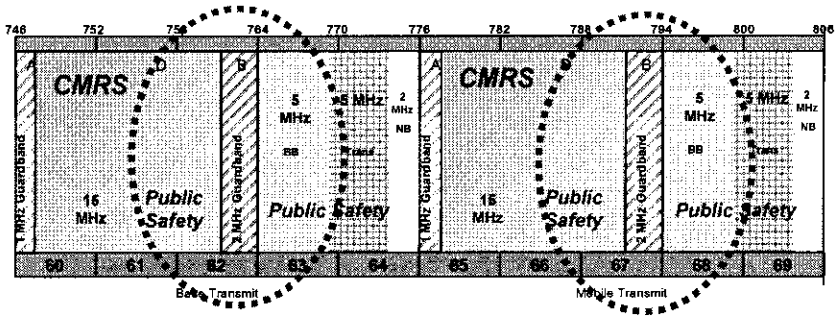

Figure 9 – Rechannelization of lower Public Safety band

Phase 2b – Evolve from a "split" narrowband approach (Narrowband on Upper and Lower portions of band) to consolidate Broadband on lower frequencies (thus matching the technology below 764 MHz).

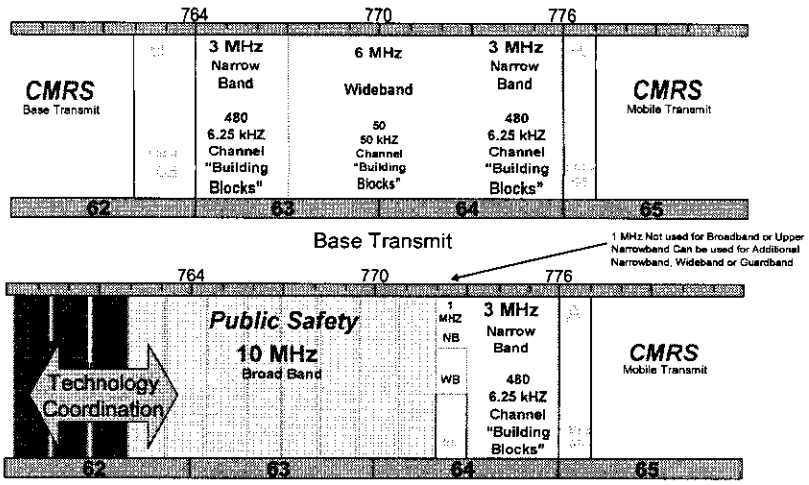

Figure 10 – Rechannelization of lower Public Safety band

Phase 3 – As Narrowband technology demand wanes at its own pace, unused spectrum can be reclaimed by broadband technologies, eventually eliminating the need for Narrowband/Broadband Guard Bands. A Guard band to separate base station transmitters from mobile receivers may still be required.

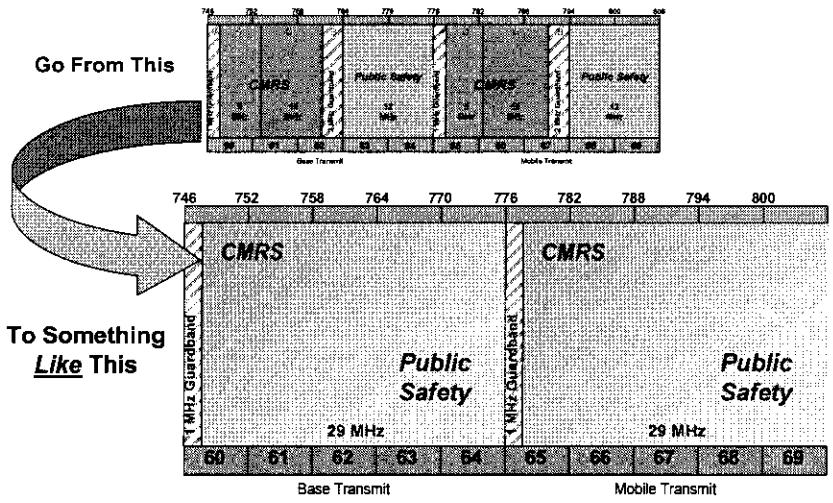

Figure 11– Increasing spectral efficiency by spectrum sharing

The optimal way to secure future flexibility and capability is to allow Public Safety, should they desire and require it, to share portions of their 24 MHz allocation, with the combined "C&D" blocks. This allocation should be sufficient spectrum to justify a cost effective, high capacity, high functionality for Public Safety, which can be shared with a commercial entity (ies) and still deliver viable economic results.

Demands for Public Safety spectrum are already claiming that the 24 MHz allocation is insufficient, particularly the way it is currently channelized[23], and this is just for day to day operations. When consideration is given to the needs of the Public Safety community during a critical incident, these needs escalate rapidly[24]. To fulfill critical incident needs Public Safety must have access to spectrum to allocate quickly and easily (which the new network could support) and this cannot be spectrum currently allocated as part of the 24 MHz. Figure below shows the proposed public/private spectrum sharing fully meets this need in a flexible manner dynamically allocating the resources where they are most needed.

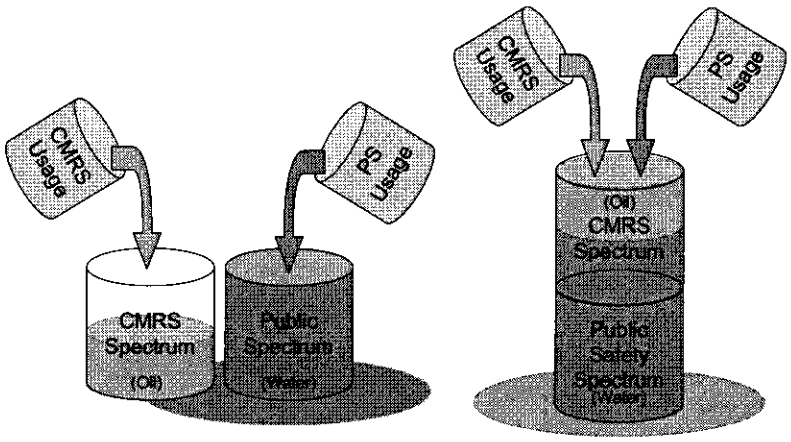

Figure 12 - Efficient allocation of spectrum resources

Emerging technologies have capabilities, which are better than those of today's Public Safety technologies; and are more spectrally efficient, cost effective to deploy and better suited to handle bandwidth and service allocations in the events of a critical incident. However, in order to fulfill the basic needs Public Safety needs more than 24 MHz. APCO states that 90 MHz are required to provide broadband applications for Public Safety[25], project MESA conducted an analysis that concluded that to provide service to over 300 first responder entities in the same cell 70 MHz will be required[26]. Adjacent spectrum would be the logical choice. Finally, given all of the demands of

---

[23] SPECTRUM NEEDS OF EMERGENCY RESPONSE PROVIDERS comments in response to the Commission's *Public Notice*, FCC 05-80, released March 29, 2005, WT Docket No. 05-157

[24] See Project MESA document: Train Crash Scenario – draft spectrum assessment example – by Steffen Ring

[25] SPECTRUM NEEDS OF EMERGENCY RESPONSE PROVIDERS comments in response to the Commission's Public Notice, FCC 05-80, released March 29, 2005, WT Docket No. 05-157

[26] See Project MESA document: Train Crash Scenario – draft spectrum assessment example – by Steffen Ring

Public Safety – it is inconceivable to think of a viable business case for the commercial entity with anything less than a 30 MHz allocation.

6.2 Coverage

The bulk of the radio coverage will be delivered through a network of communication towers. This radio network will be designed to provide reliable and broad coverage and sufficient capacity for all but the most catastrophic emergency.

The radio network design will ensure that all but the most rural areas will have terrestrial coverage and the most advanced services possible with that coverage. The 700 MHz spectrum is ideal for providing broadband, mobile, wireless coverage. The frequency translates to reasonable gain antennas that fit within a mobile device form factor (1/4 wave antennas would be approximately 4 inches), more importantly the frequency band has good propagation characteristics. The Figure below[27] depicts how the path loss decreases in a moderate urban area as a function of frequency; also shown how the path loss decrease can have a significant impact on the geographic coverage.

[27] Calculations were based on moderate urban environment utilizing the Hata (for 700-1500 MHz) and the extended Hata (for 1500+ Mhz). Models were obtained from the National Institute of Standards (NIST) website. Note: The Extended Hata model shows better link performance than reality for frequencies above 2000 MHz

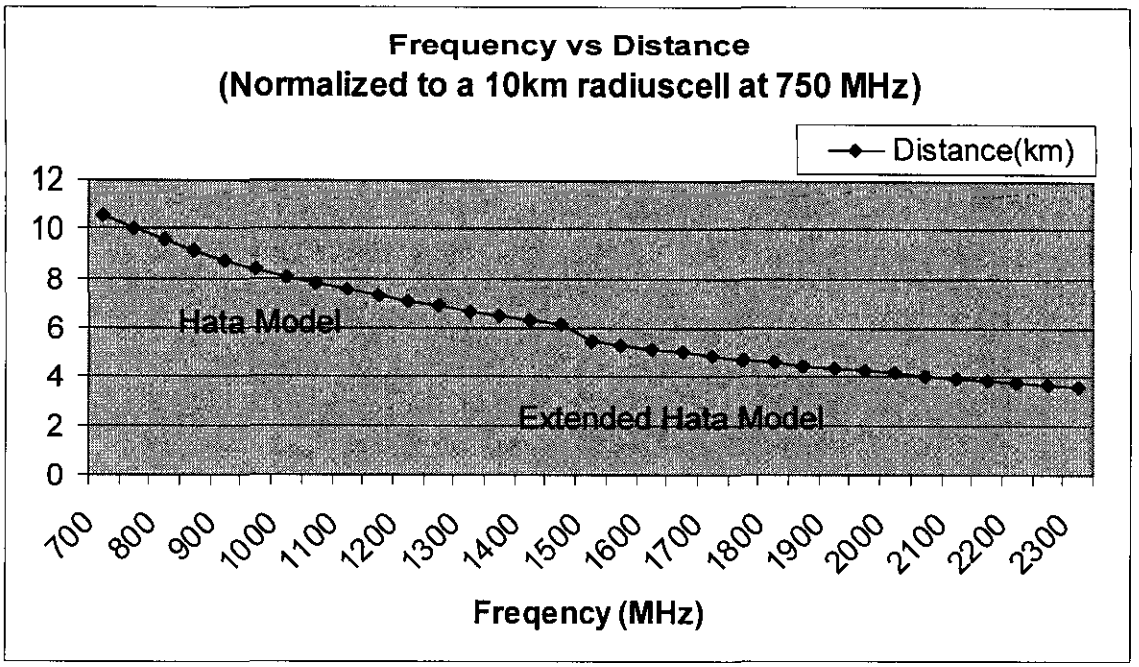

Figure 13– Cell Radius as a function of Frequency

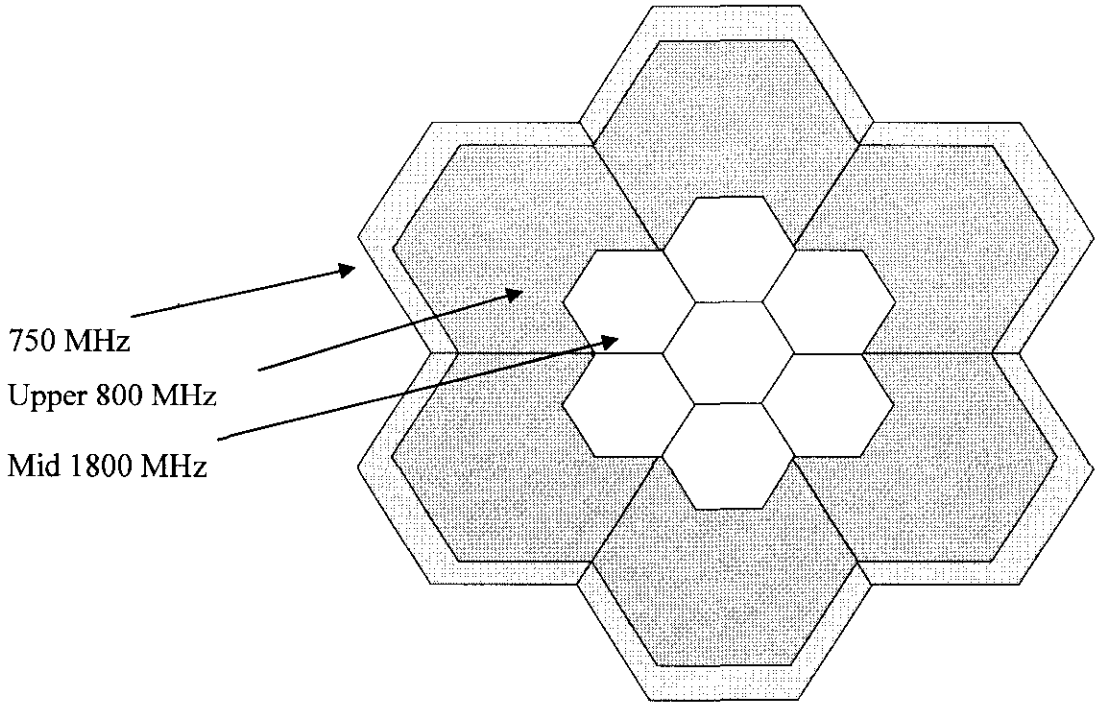

Figure 14– Geographic Coverage Comparison for Moderate Urban Environment

For the same reliability and geographic coverage, 700 MHz will result in fewer base stations; however, the Public Safety system cannot operate at the same reliability as commercial systems. It is critically important that Public Safety has access to a system with reasonable propagation characteristics as the reliability requirements of Public Safety will significantly impact cell coverage as shown in the figure below.

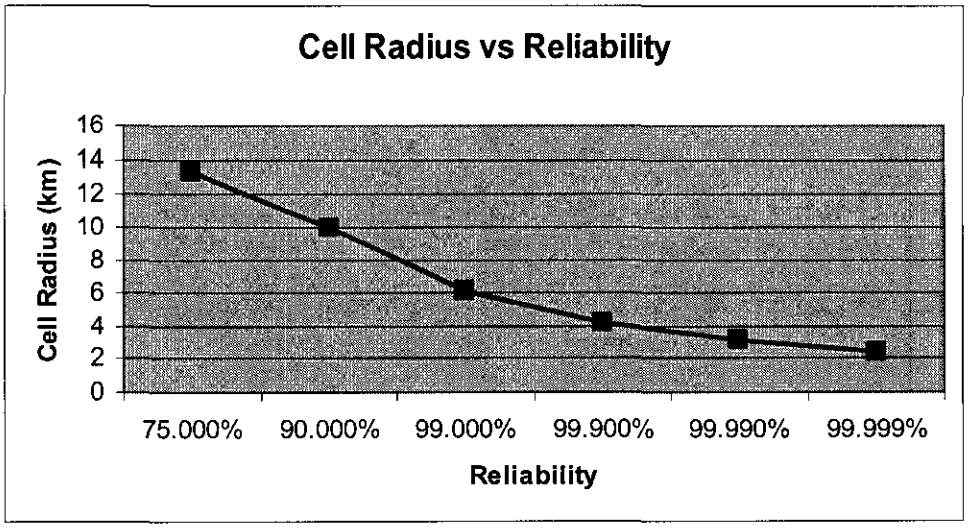

Figure 15 - Cell Size as a function of Reliability

From a coverage perspective, 700 MHz is an ideal band for Public Safety. It can provide reliable coverage more economically than any of the higher bands, and it is sufficiently high frequency to support small devices that can leverage off the developments of the commercial and public safety devices in the 800 MHz band.

In addition to terrestrial coverage, other methods will be used to ensure Public Safety first responders have coverage when and where they need it. These include using mobile vehicle systems to enhance and/or extend coverage by relaying portable radio communications to the network. It is envisioned that these system could be integrated into the communication systems of existing first responder vehicles, as well as be specially designed as rapid deployable communication assets.

Additionally, a satellite overlay system will be integrated into the Next Generation Public Safety network to provide an additional layer of coverage. This system is discussed in greater detail in section 6.5 Satellite Overlay.

6.3 Reliability

Reliability as it is used here is defined to be the ability for users to use the network's services. Reliability requires all components of the network to work in conjunction to deliver the services to the end user.

- Radio
- Network

- Application
- Services
- Device

Radio Reliability

One component of reliability is coverage. As mentioned above, to achieve greater radio link reliability the density of communication towers must increase. The network must be designed such that not only is there coverage, but that it is overlapping and redundant to ensure that no single point of failure exists.[28] It is likely that it will not be economical to provide 100% reliable coverage with redundancy, solely through a fixed terrestrial network; however, the network will have many mechanisms to ensure that the radio system is as close to 100% reliable as possible. First, the terrestrial radio network will be designed to a higher grade of service than the commercial systems. Thus in a fully operational system, there would be few locations that did not have coverage. Also, this dense coverage provides a layer of redundancy in the event of a communication tower outage. In most cases, an urban/suburban area outage would not result in loss of coverage, but it may result in reduced reliability in buildings and elevators or reduction in available capacity. Not only will there be dense coverage, the radio systems will be hardened and provided with additional redundancy. It must have redundant, off grid power capability (such as generators), multiple and redundant connections from the radio system to the network, the ability for a radio site to continue to provide coverage even in the loss of network connectivity, and enhanced physical security.

However, given the fact that there may be areas where coverage is lacking either due to a system outage, or incredibly harsh radio environment, the system will have the capability of deploying mobile transmission facilities. These facilities could either fill in during a system outage, or be deployed to provided additional coverage where needed. Additionally, there must be a Satellite Overlay network to provide coverage as well (more on this system is discussed later). Finally, the Public Safety user would always have access to their Personal Area Network[29] regardless of the communication state of the network at large.

Network Reliability

[28] Network Functional Requirements from "Statement of Requirements for Public Public Safety Wireless Communications and Interoperability", The SAFECOM Program, Department of Homeland Security, Version 1.1, January 26, 2006

[29] Network Functional Requirements from "Statement of Requirements for Public Public Safety Wireless Communications and Interoperability", The SAFECOM Program, Department of Homeland Security, Version 1.1, January 26, 2006

Network Reliability is the network being operational and fully capable of performing its functions. To achieve high standards (99.999%) of reliability several mechanisms will be used in the NGPS. Platforms will be hardened, communication paths will be redundant, and functional nodes will be distributed such that there will not be a single point of failure in the network. The end result is a network that will reliably deliver content.

Application Reliability

In addition to the network and radio systems, the applications themselves must be reliable. The NGPS will accomplish this by ensuring application platforms are 99.999% reliable (the hardware and software systems that applications "plug-in"), and by creating a framework such that applications can be geographically distributed, yet still provide seamless service.

Service Reliability

The supporting functions of the radio, network and applications are the first step in providing end to end Service Reliability, however there is additional steps that are required. End to end priority and class of service management schemes will be in place to ensure high priority services are never impacted by lower priority service behavior. Additionally, service interactions will be managed such that activity in one service does not preclude activity in another service (an example would be receiving a PTT call while in a Voice call, the NGPS will ensure that the user has the option to take the PTT call, or deliver it to an alternative destination, whether another user or a voicemail-like system.

Device Reliability

Devices for Public Safety must be reliable. It is the interface to the end users and must provide the user with services when and where needed. Creating devices that can sustain the rigors of first responders requires a holistic approach. The physical housing and controls must be sturdy and able to sustain innumerable environmental conditions. The circuitry and electronics must be immune to impacts and must also have adequate protection from wet, smoky, hot, cold, etc. environments. Software must be rigorously tested to ensure that it is stable and consistent. Additionally, the user interface must be simple to use and understand, and be proof against human confusion and errors.

6.4 Capacity on Demand

The radio network is shared among many constituents, the most defining being Public Safety and Commercial Interests. Although at first glance this would seem to be competing interests for the same resource, it is possible for both segments to coexist and even benefit from characteristics of the other.

By designing priority based classes of service associated with quality of service metrics into the network, it is possible to create an elegant system where Public Safety has on demand access to the full resources of the system, while the Commercial systems are free to utilize any unused capacity. Furthermore, this relationship is improved by the usage pattern of the two domains. Public Safety needs capacity based on worst case scenarios, but rarely utilizes the system to that capacity. Commercial interests can take advantage of this unused capacity without impacting Public Safety communications.

This situation is further enhanced by improvements in technology that allow the creation of one large shared "pipe" or throughput, versus many smaller pipes that have to be individually managed. With a single channel, the system control mechanisms are focused on managing user flows, rather than managing channels to user types.

Figure below shows how capacity and bandwidth aggregated in a conventional approach:

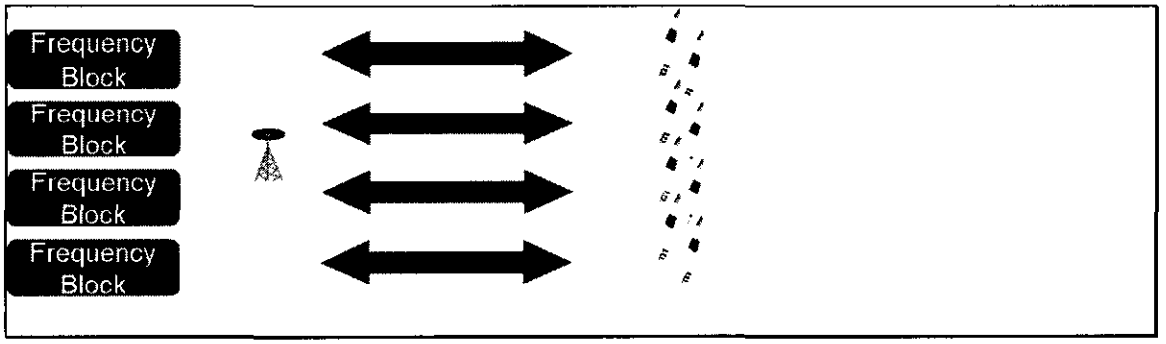

Figure 16- Conventional Frequency Aggregation

In contrast, depicts how pooling frequency blocks increases higher bandwidth and less congestion.

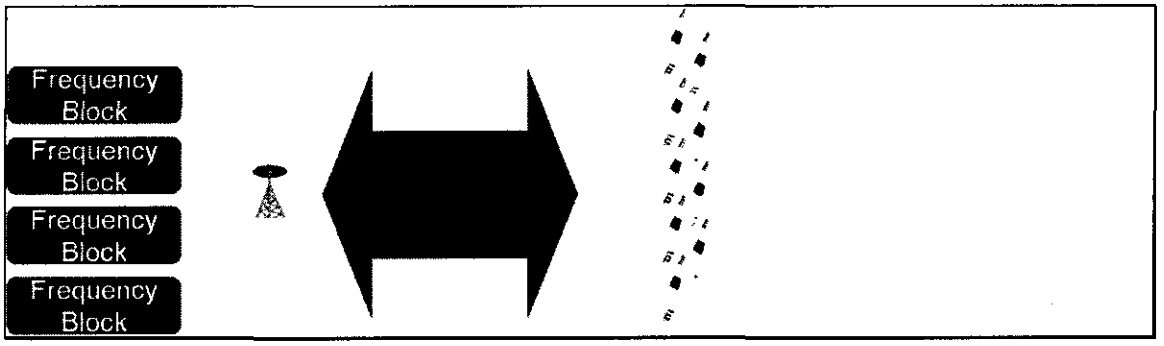

Figure 17 - Pooling Frequency Blocks

Pooling resources mitigates congestion issues, but does not eliminate it. Other mechanisms must be in place to ensure priority users have access to capacity when they

need it. In order to ensure access to priority services and users, there are two issues that need to be addressed. One is ensuring that priority services are not delayed by network congestion. The second is that priority services and users can access the network in congested conditions.

First, to prevent priority services or users from being delayed by congestion, these services and users will be assigned higher priorities. These higher priorities translate into specific priority markings on the individual internet protocol (IP) packets. One advantage of having a collapsed network to all IP components is that these priorities can be globally enforced throughout the system. An example of how priority will ensure expedited delivery of important services is shown below:

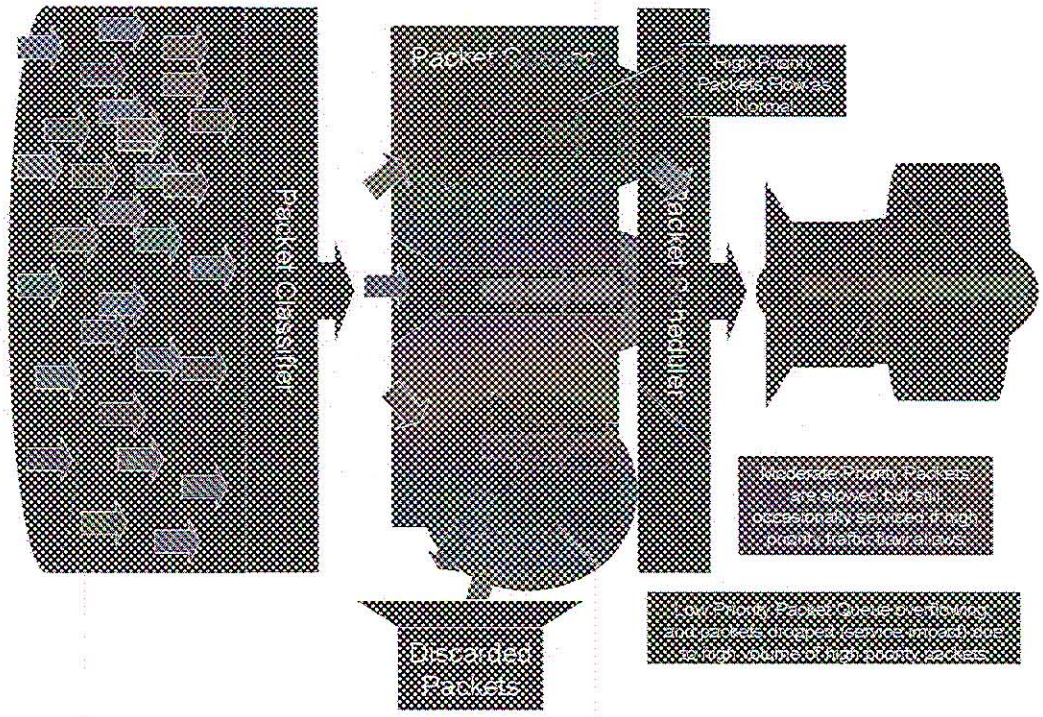

Figure 18- Quality of Service Management

Achieving the appropriate segmentation between user bases, it is accomplished by marking packets and sessions with Class of Service and Priority of Service where the entire network is designed to enforce those markings in a consistent way. Most technologies have the capability to assign priority to packets, but what is necessary is the rule-set that assigns the appropriate priority to the various packet flows. In the NGPS network, this function is part of the Command and Control aspect of the network, and is closely linked to service management (see also Services and Command and Control sections).

An example for priority assignment would be a hierarchical management interface. A jurisdiction would assign priorities to the radios and services that are important to them, as well as indicating those services that would be critical in an

emergency. The system would then register the devices and services with these priorities and ensure that all the session and transport elements would enforce that priority. Public Safety would have higher QoS settings than Commercial, so in resource contention situations Public Safety would be insured highest priority. In the event of a lack of resources, Public Safety would pre-empt Commercial users. This results in a network that behaves dynamically and appropriately to insure the needs of Public Safety pre-empt commercial needs (see figure 10 for a visual representation of this concept). Nevertheless, if there is still sufficient capacity, the commercial users will still be free and able to access their normal functions.

Another aspect that must be considered is the granting access to the network. Quality of Service mechanisms can work well in shaping and controlling traffic, but they do not address controlling access to the network. This can become critical at the wireless base stations if there is a flood of access requests coming in. Qualities of Service mechanisms don't help in this situation, since the messages need to be processed first in order to determine how they are to be treated. To prevent unnecessary congestion during periods of high Public Safety demand, the NGPS network must slow down; and perhaps in some instances even have the capability to stop low priority devices from accessing the network.

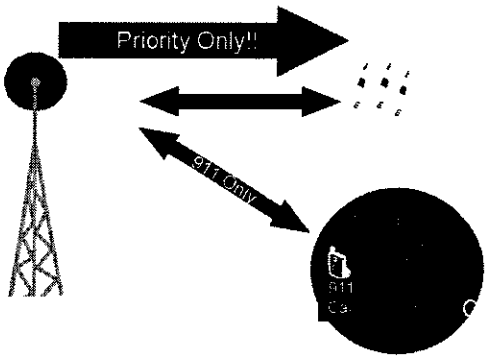

Figure 19- Radio Access Control

It is expected that there will be multiple levels of control, to ensure that high priority users always maintain access to the network. The table below highlights possible scenarios.

Table 4 – Radio Access Procedures

Situation	Action
Normal Operation	Normal Access Procedures
Congestion	Low Priority Users use extended backoff algorithm for access
Emergency	Low Priority Users use extended backoff algorithm for access
Congested Emergency	Low Priority Users prevented from accessing the system. High priority users go into extended backoff algorithm that varies according to priority

6.5 Satellite Overlay

The Public Safety network must overlay the terrestrial coverage with satellite provided coverage. This will provide an additional layer of redundant communications that could provide contingency coverage in the event of terrestrial network outage. The overlay would also provide a layer of coverage for rural areas with limited accessibility.

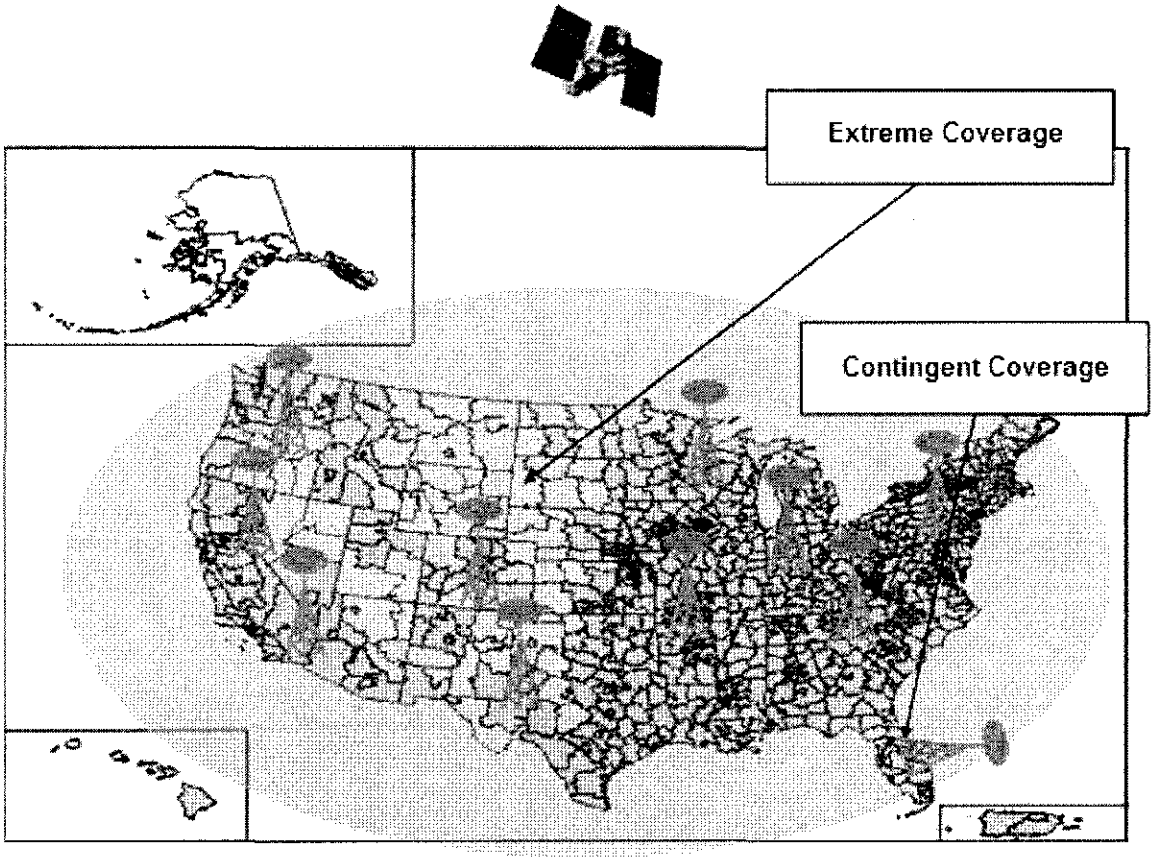

Figure 20- Satellite Overlay

This overlay would be accomplished by having a Mobile Satellite System (MSS) coupled with the NGPS Terrestrial Network. This architecture is similar to systems and concepts proposed to the FCC previously[30].

[30] "Application for Assignment of Licenses and for authority to Launch and Operate a Next-Generation Mobile Satellite Service system," filing to the FCC, filed by Motient Services Inc. and Mobile Satellite Ventures Subsidiary LLC, January 16, 2001 and Flexibility for Delivery of Communications by

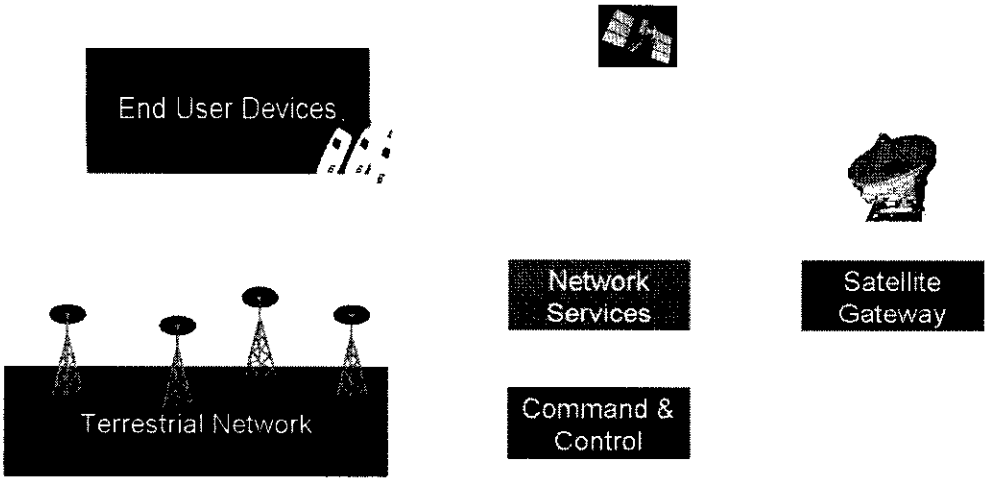

Figure 21 – NGPS with Satellite Component

As mentioned, the Satellite Overlay would provide additional robustness to the network; however there are some limitations to the satellite provided component. Traditional satellite orbits introduce significant delay of 200-500 milliseconds. Real-time, interactive services may be affected by that delay and will need to be managed effectively.

There is also the issue of capacity. Advances in antenna systems and other technology have increased the capacity capabilities of satellites; but due to large geographic coverage areas, total bandwidth requirements will have to be managed. However, the advantages of having a communication system that overlays a terrestrial network outweigh the limitations of current generation satellite networks. Furthermore, it is fully anticipated by the time that a Public Safety network deployment could commence, there will be sufficient advances in satellite and ATC technology, which can help mitigate these issues.

The Public Safety network must be designed to integrate Satellite coverage as seamlessly as possible into the overall network. However, there will need to be active management over service access for Satellite users to ensure that Satellite users can effectively use features and services to the maximum extent possible given satellite network constraints, and that Satellite users do not degrade the capabilities of terrestrial services and applications.

Mobile Satellite Services Providers in the 2 GHz Band, the L-Band, and the 1.6/2.4 GHz Bands; Review of the Spectrum Sharing Plan Among Non-Geostationary Satellite Orbit Mobile Satellite Service Systems in the 1.6/2.4 GHz Bands, Report and Order and Notice of Proposed Rulemaking, IB Docket Nos. 01-185 and 02-364, 18 FCC Rcd 1962 (2003), petitions for reconsideration pending ("ATC Report and Order", modified sua sponte by Order on Reconsideration, 18 FCC Rcd 13590 (2003), ¶ 2, 20-45, 210-11.

6.6 Services

A service is defined as the network taking an action on behalf of a user or other end-point. Closely related to "service" is the term "application", although often used interchangeably the terms have different meanings. An application is the logic and server that performs a specific function. A service comprises all components of the system that are needed to deliver the service, including interacting with other applications and various capabilities latent in the infrastructure and devices. An analogy would be house and neighborhood. The physical aspects of the house and how it relates to you is similar to an application. The house in conjunction with the neighborhood would be analogous to a service. Building a house would require plumbing (application), but it does not include ensuring the water pressure is sufficient for utilizing the plumbing (service). A network example could be a PTT Application, which is comprised of client and server systems that process PTT messages. A PTT service is the entire system for delivering and receiving PTT calls, plus the way PTT effects, interoperates, and co-exists, with other applications and services.

In the NGPS network there are three categories of services: general services, specialized services, and commercial services. Commercial services are those that are offered on the commercial users in the network. They fall under the purview of the commercial operator. It is expected that the commercial operators would offer typical wireless and broadband services. For Public Safety, there are general services and specialized services. General services are those services that can be implemented throughout the network, across all logical networks, and are capable of interoperating or being inter worked with critical external networks (such as a legacy Public Safety system). There are two categories of general services; those services offered across the entire network plus any interoperating networks, and those services that are offered across the entire network. This hierarchy is depicted in Figure 22 below:

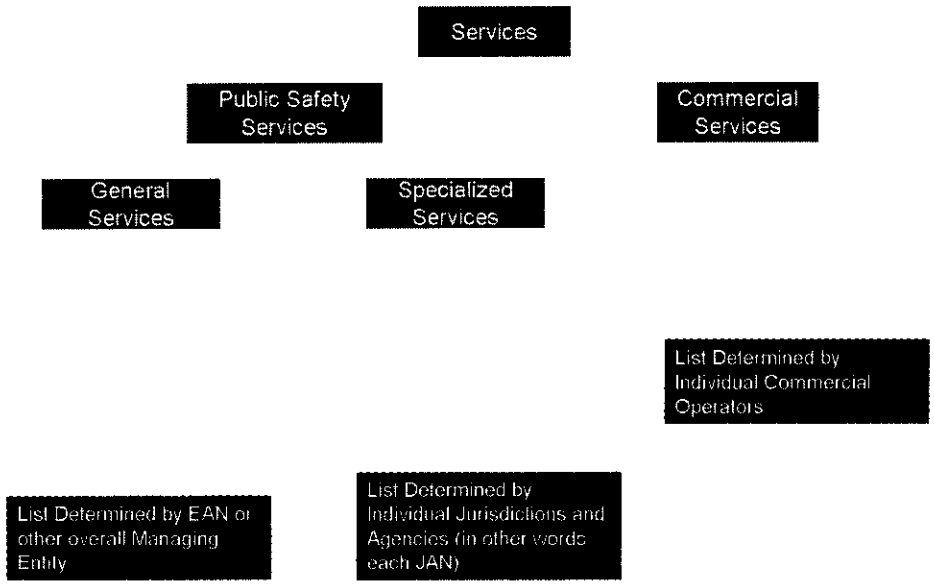

Figure 22 - Service Control Hierarchy

Specialized Services are those services that offer additional capability that may be required by individual jurisdictions or agencies that are not offered by the Extended Area network at large.

The difference between a general service and a specialized service is less a technological distinction, and more one of policy, definition and implementation. If all agencies have a service capability and implement it in similar ways, then that service can and should be considered to be classified a general service. Initially general services would include Push-to-Talk, Full Duplex Voice and perhaps basic data access. Advanced Services opportunities are virtually unlimited. To allow for consistency, a Services Framework will be created to ensure that Public Safety agencies can implement independently services that fit their needs, yet ensure those services are scalable and adoptable to other agencies that have similar needs. The framework would allow for rapid adoption and integration of new services.

Framework and Process

The service capabilities of the NGPS network should not remain static, however, it is critical that services are stable and reliable. To this end a framework would be developed that would allow services to be able to migrate from their point of adoption (whether commercial or Public Safety) to become applicable to the network at large.

The framework will ensure the service addresses the needs of Public Safety, while issues such as stability, reliability, scalability, interoperability, serviceability, manageability, etc. are verified. Once validated the service could then be offered to the entire network as a new interoperable feature. There are three ways that a new service could become part of the larger network. The first is through allowing individual jurisdictions to implement solutions specific to their needs, and through a best practices framework, the larger network can adopt those systems that have been field proven. The second is through a rapid commercial adoption program. Services that are offered on the commercial network can be leveraged into the Public Safety network, although additional testing and validation would still be required. The third option is through direct development. If a critical need is unaddressed by commercial off-the-shelf products, nor is there any existing service, it would be possible to introduce new services through a technology development process. This process would be similar to commercial practices, with the exception that more rigorous testing and validation would be required before the service went into the network.

Service Differentiation

It is expected that the network will have a host of services, and that there will be times that services will need to compete for network resources. To ensure that services operate at peak efficiency, a mechanism to differentiate and prioritize services is

required. Mechanisms for this have been suggested in existing Public Safety requirements documents[31]

Leveraging the work of these documents, services would be categorized by the following characteristics: Timing, Interaction, and Priority.

Timing	Interaction	Error Tolerance	Priority
Instant/Real-Time	Interactive	Error Tolerant	Emergency
Time Sensitive	Non-Interactive	Error Intolerant	Mission Critical
Time Insensitive			Normal
			Low

This categorization results in 48 possible categories. Other Public Safety documents generally categorize services into fewer categories; however, it is possible to provide a mapping. A mapping to SAFECOM Classes of Service for example:

Class of Service 5 – Low Priority/Best Effort

- Time Insensitive and Low Priority

Class of Service 4 – Low Loss (file transfers)

- Non-Interactive and Error Intolerant
- Not Instant/Real-time and Not an Emergency or Mission Critical

Class of Service 3 – Interactive Applications (Instant Messaging, Database queries)

- Interactive
- Not Time Insensitive and Not Emergency or Mission Critical

Class of Service 2 – Highly Interactive (Session Signaling)

- Interactive
- Not Time Insensitive and Not Low Priority

Class of Service 1 – Real-time, Jitter Sensitive, Interactive

- Instant/Real-Time and Interactive
- Not Low Priority

Class of Service 0 – Mission Critical Class 1

- Emergency or Mission Critical

[31] Most notably SAFECOM and Project MESA

- Not Time Insensitive

Network Control

These Service Categories would be mapped to Quality of Service metrics and enforced in the network, utilizing some of the same mechanisms to provide Capacity on Demand for Public Safety.

Classifying packets into the appropriate queue assists in addressing two of the service classifications: Interactivity and Error Tolerance. Interactive sessions need to be assigned to a queue where the likelihood of losing the information is low (longer queues), while error tolerant packets could be assigned to shorter queues with no degradation to the service. The packet scheduling addresses the other two service classifications of Timing and Priority. Priority packets and those with stringent timing requirements would be sent to a queue that would be serviced more often.

6.7 Interoperability

The Public Safety community requires interoperable communications, which is the ability to communicate and share information as authorized when needed, where needed, and in a mode or form that allows the practitioners to effectively use it. Broadly defined, the Public Safety community performs emergency first response missions to protect and preserve life, property, and natural resources and to serve the public welfare. Public Safety support includes those elements of the responder community whose primary mission might not fall within the classic Public Safety definition, but whose mission may provide vital support to the general public and/or Public Safety officials. Law enforcement, fire, and EMS fit the first category, while transportation or public utility workers fit the second.

Interoperability can take many forms. As discussed here, interoperability is between an user on a legacy radio operating on a legacy system communicating with a new user operating on the new system via system to system communications. Specifically not addressed is a legacy radio interfacing directly with the new network, or vice versa, a new radio working on a legacy network. However, there is nothing to preclude the evolution of multi-mode devices, which would ultimately support RF roaming capabilities as well. Traditionally, these requirements contribute significant complexity and therefore cost to the devices.

To achieve communication interoperability with legacy systems, two things are needed. First, an interface provided by the legacy system for legacy access. This interface can take several forms, but without access to the legacy system, interoperability will not be possible. Second, the new system must provide an interface and mechanisms for interoperability. Not only must there be a physical interface, there must be the logic and control functions that associate legacy and new system components together. The Public Safety network can provide the second set of capabilities, it is expected that legacy systems that wish to be interoperable provide the appropriate legacy interface.

Interoperability would be achieved by creating the associations and connections between the legacy Public Safety interoperability interface and the NGPS system. To achieve the maximum level of interoperability, the NGPS system would mirror the capabilities of the legacy system, and inter-work those capabilities into the features and functionality that exists on the NGPS.

6.8 Devices

The Device component includes all functions that originate or terminate within a system that is external to the network, yet reliant on the network to provide some measure of capability. The Device component is separated into two parts. The Device Network, which discusses Device Connectivity, and the Device Functions, which discusses the functional aspects of the Devices.

Device Network

In the Next Generation Public Safety Network, networking will extend to the device. SAFECOM produced an interface diagram that shows one implementation of this concept.

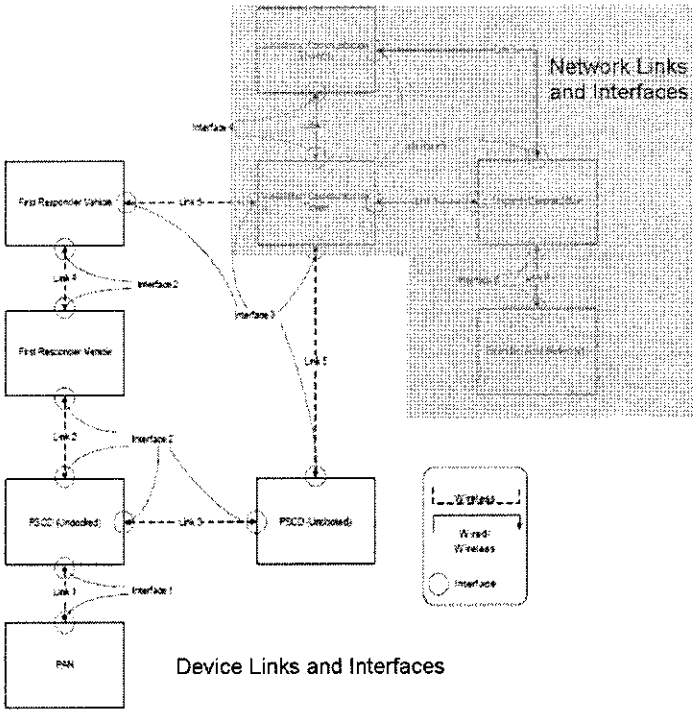

Figure 23 - SAFECOM Device Interfaces

The Next Generation Public Safety Network Implementation View is depicted in the figure below.

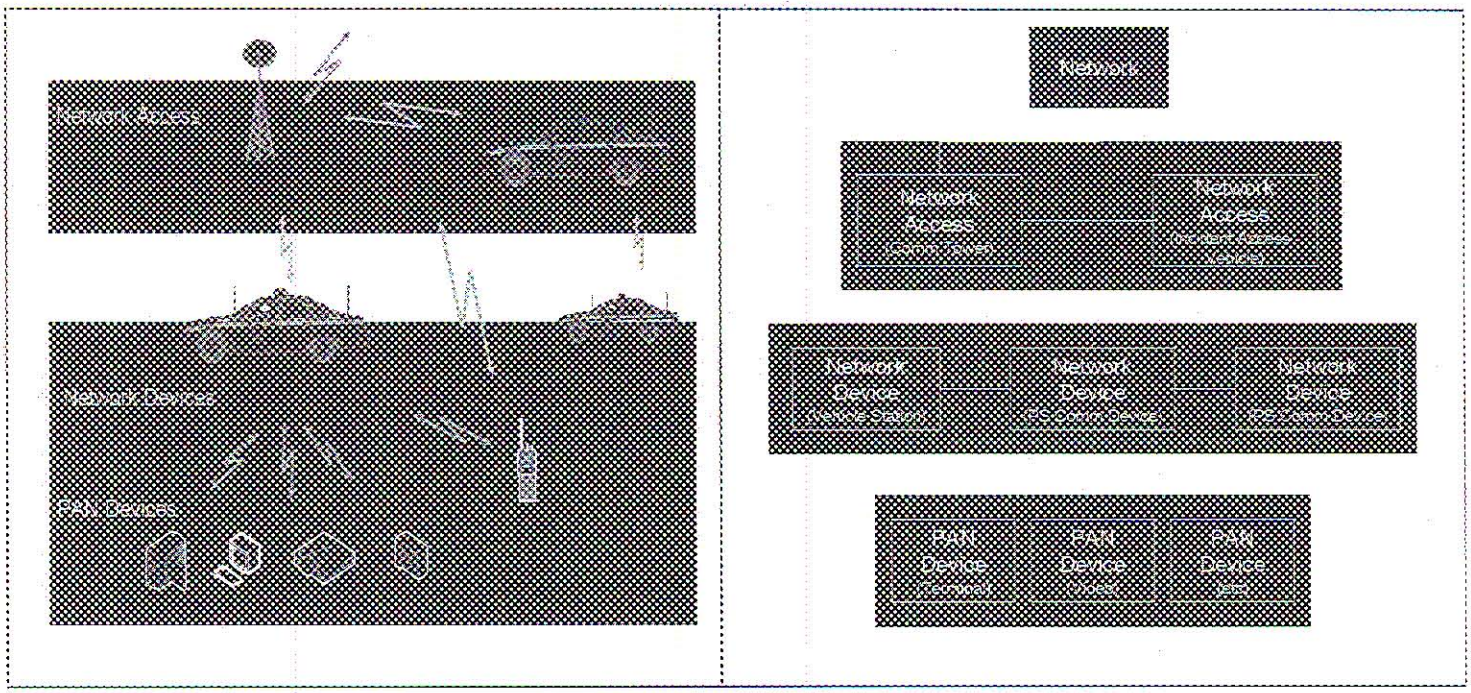

Figure 24 - Device Connectivity

The views are quite similar, the notable exceptions being the ability for a PAN device to have an interface with the Vehicle Station, and the creation of a separate interface for a vehicle that is acting to relay traffic to the network (such as in an incident). In effect, the vehicle in this configuration is acting as a mobile communication tower, that is relaying the network traffic wirelessly to the network (through a fixed communication tower or a satellite link), rather than a traditional mobile communication tower, often referred to as a "Cell on Wheels" (COW), which uses a fixed (typical wireline) method to access the network.

Device Functions

There are four main categories of device: Network Device, Vehicle or Portable Device, Autonomous Device (sensors, video cameras, etc) and PAN Device. Each category has different functional needs as highlighted below:

Figure 15 - Device Functions

The NGPS network device approach will be to develop devices that meet the composite needs of Public Safety. This requires a vastly different approach to device specification, design and implementation on the part of the core technology (microprocessor and software) providers and outside equipment manufacturers (OEMs.)

Device development must begin with the air interface selection and the identification of any unique enhancements required for Public Safety needs. The next step in the process is analysis of the device operating system, runtime environment for applications, services and advanced networking capabilities. Finally, the stringent requirements regarding user interface ergonomics, durability, battery-life, etc. must all be taken into consideration for impact on the final design.

Device development represents an interesting opportunity for the incumbent Public Safety technology companies to collaborate with the commercial technology enterprises. Public Safety device manufacturers have a long history of developing technology that is ergonomically tailored to Public Safety users. However, they are not accustomed to working with the advanced technology capabilities inherent in emerging commercial solutions. Melding these two sets of experience should yield compelling results.

The goal of NGPS network device design must be to include all advanced capabilities inherent in the emerging commercial technologies, without sacrificing any ergonomic customization required for Public Safety. Furthermore, a sophisticated

framework for managing service interaction in Public Safety devices must be a priority for the industry.

6.9 NGPS Logical Networks

The physical NGPS network must be designed to operate as multiple logical networks. Having a system operate on logical networks provides tremendous flexibility and control over the network topology. Advantages of this approach are: the ability to create additional levels of hierarchy, the ability to reconfigure the logical networks in time of need and the ability to distribute control of the network.

The partitioning of the network can be structured according to the following scheme:

An initial partition would segment the network into a Public Safety network and a Commercial network. The network segmentation would be configured such that the network capacity sizing would be dynamic. Public Safety would have user access priority and would be able to access the full capacity of the network. The Commercial network would have access to any capacity that is not set aside or being utilized for Public Safety. Given that the network MUST be able to support the large capacity needs of major emergencies at any given time, there must be significant capacity overhead. In a traditional network this overhead would go unused. However, in a logical segmented network, the unused capacity could be utilized by day-to-day commercial interests without impact to the communication capabilities of Public Safety.

Each of these two logical networks, the Public Safety and the Commercial, can be further divided into logical networks. The Public Safety network would be partitioned in accordance with SAFECOM recommendations into an Extended Area Network (EAN), Jurisdictional Area Network (JAN), Incident Area Network (IAN) and Personal Area Network (PAN), with the logical inter-relationships defined in the following diagram.

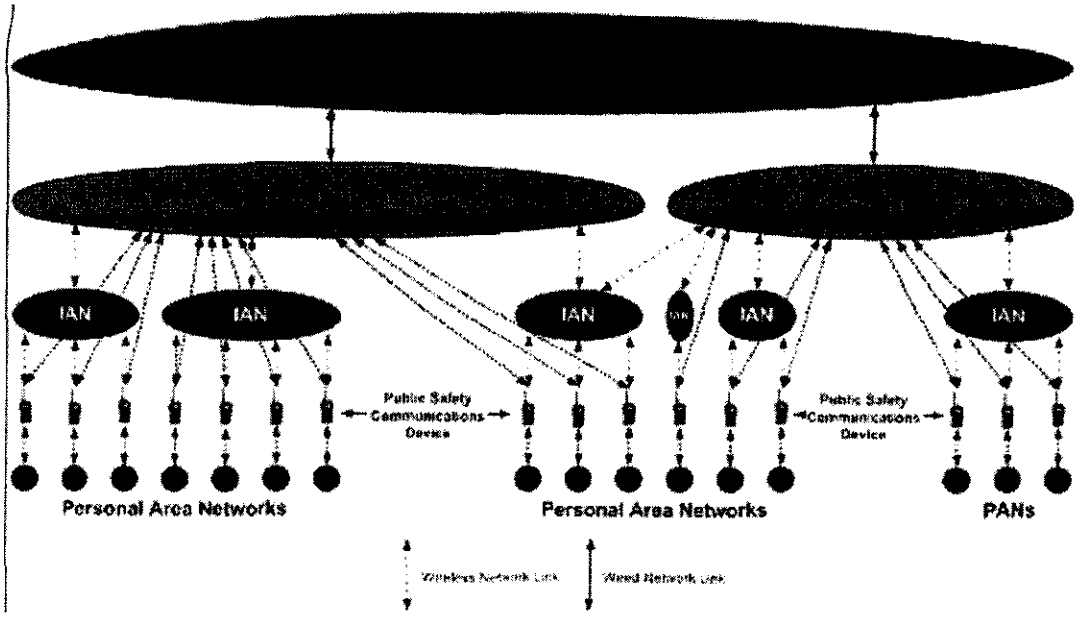

Figure 26- Natural Network Hierarchy as defined by SAFECOM

The over-arching Public Safety segment would be analogous to the SAFECOM Extended Area Network (EAN). The EAN would be comprised of various Jurisdictional Area Networks (JAN). Each JAN would map to a jurisdictional communication system, with each jurisdiction maintaining operational control of its network segment. The integration of the satellite and interoperability components of the network could be treated as a discrete JANs.

Each jurisdiction would be able to segment its networks further to meet their particular needs. It would be possible to segment the network topology down to an individual level, referred to by SAFECOM as the Personal Area Network (PAN), however it is expected that the majority of jurisdictions would not segment to that level, and that PANs would be managed at the user level, not at the network level. An analogy would be internet routing. Although it is possible to build routing tables to the individual computer level, most organizations would configure their networks to an organizational or departmental level, and the network is shared from that layer down. Other tools rather than routing topologies are then used to manage individual users and resources.

A critical logical network needed by Public Safety that has not yet been discussed is the Incident Area Network (IAN). This network would be a virtual network that would tie together multiple jurisdictional users into a single, seamless network for the duration of an incident that required response from multiple jurisdictions and/or Federal agencies.

Note that the IAN is a special type of logical network that can cross and intersect multiple other logical networks. This has the advantage that in a shared Public Safety/Private network, Public Safety jurisdictions have the capability of including Commercial entities into its Incident Area Network. The control and configuration of the IAN is by providing an Incident Commander specialized control via Access Control

functions, and provides the ability to dynamically create a virtual interoperable communication network in response to the incident.

The hierarchical levels define increasingly complex communications interactions and administration as the hierarchy moves from the single discipline/single jurisdiction situation to the multiple disciplines/multiple jurisdictions events. The level or hierarchy of the communication interaction should not cause confusion and frustration for the first responder. The first responder must be able to respond and react to each level without regard to the communications requirements and the communications functionality must be invisible to the first responder. Additionally, the first responder must be able to move seamlessly and transparently from jurisdiction to jurisdiction with no interruption in service, provided the user is authorized as local policy dictates.

Public Safety intra-agency interoperability is needed for the following communications: Day-to-Day, Task Force, Mutual Aid.

6.10 Command-and-Control

The network will be designed so that the control of the system (i.e. software "locks and keys") is capable of being distributed geographically and/or functionally. Every logical domain would have the capability of having this control, and can choose to delegate it to other entities. Access Control points will provide entities with control over the logical functions that entity has access to, as well as the means to delegate control with that entity's domain. For example, the Public Safety domain would most likely have an Access Control point. Figure 27 shows the flow of control in the Next Generation Public Safety (NGPS) Network. Policies, procedures and other administrative guidelines are developed by the Public Safety Broadband Trust (PSBT). The PSBT working in concert with Commercial Interest groups provides guidance to the Command and Control Node (CN) for the overarching NGPS network. Note that this is the sole Control Node that has control over the *physical* components of the network. The remaining Command and Control Nodes maintain logical control over their domains. Another special Command and Control Node is the Incident Area Network (IAN) control node. This node is temporary in nature and is a virtual node, in that it relies on other Control Nodes to effect changes. Public Safety User Control is typically the province of the Jurisdiction Area Network (JAN) Command and Control Node. This is where user management occurs. Finally, interoperating with legacy Public Safety systems can be controlled either through the EAN CN or the JAN CN. Local jurisdiction interoperability is typically configured through the JAN CN. System wide interoperability would be through the EAN CN.

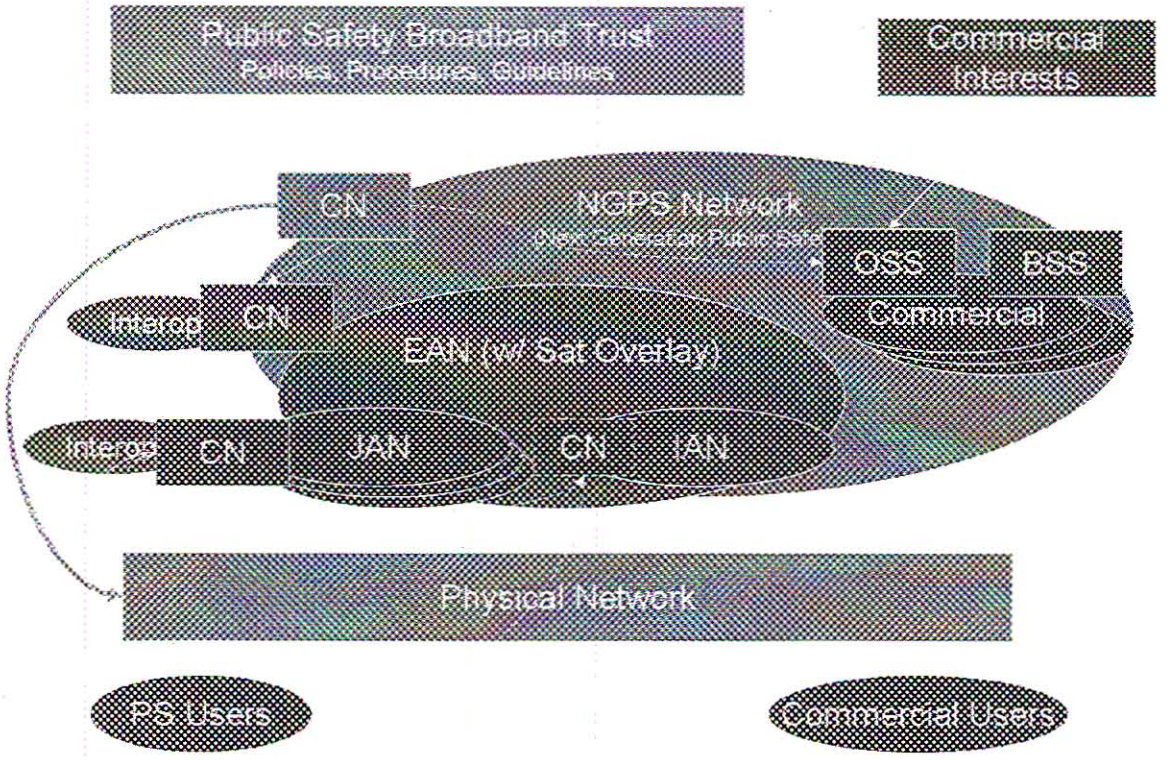

Figure 27 - Command and Control Hierarchy

Command and Control Node Flexibility

A Command and Control Node is logically separate from the physical network and the logical domain, this allows for flexibility in managing the system. A Control Node is needed for each logical domain created, but these domains do not have to be limited to the SAFECOM specified domains. It is possible to create additional overlapping domains (similar to the IAN) and give unprecedented flexibility to organize communications systems in various configurations. Control Domains can be organized by geography, jurisdiction, task force, or by function (i.e. a domain for all Infectious Disease first responders).

To create a new logical domain, one must determine the parent domain, assign the resources to be controlled by the new CN node (resources can be from any domain), and assign capabilities that the CN node is capable of managing (capabilities cannot exceed that of the parent domain). Note that managing resources that are not under the span of control of the parent domain will requires that the CN node directly responsible for those resources has let them be "assignable" to other domains.

Command and Control Node Capabilities

The Command and Control Node is a system designed to support Public Safety's Mission. At the most basic level the control nodes must assist the commander's on the

ground to quickly grasp the situation and to facilitate the implementation of assigned tasks and responsibilities, and evaluate progress

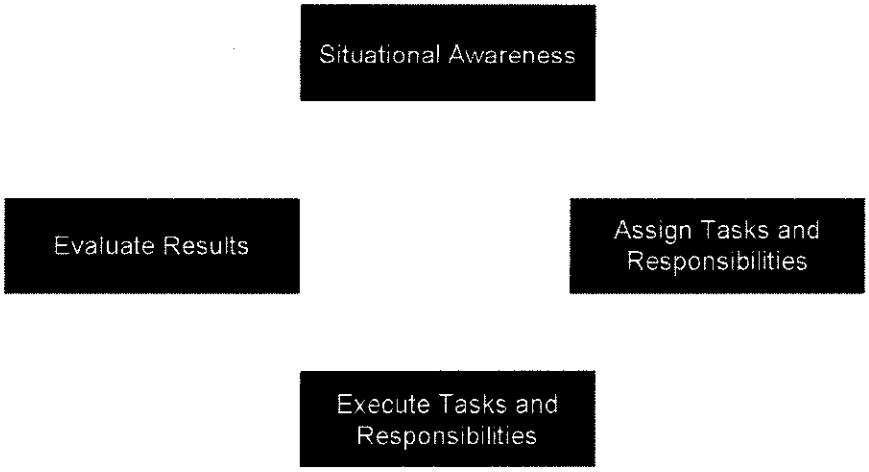

Figure 28 - Command and Control Loop

The network Command and Control Nodes need to support all aspects of that loop. From a network functional perspective, the loop can be reduced to two nodes: Situational Awareness and Evaluation, Assignment, Execution of Tasks and Responsibilities. The first are the capabilities that will inform the first responder community on all aspects of the network. The second, Assignment, Execution of Tasks and Responsibilities are the network support capabilities.

Situational Awareness and Evaluation

The Command and Control Nodes must support the Situational Awareness by being able to provide real time status on all aspects of the network as well as cataloging *capabilities*. This information should be provided on user (first responders), devices, network components, logical domains, peered systems, interoperable capabilities, etc.

The Command and Control Nodes must also be able to receive information in various formats, and be able to process that information and/or relay the information on to another Command and Control Node. Information could be either network management information or communications (i.e., video from an incident, or incident talk group).

The information must be available but also must be filtered appropriately. Data will be presented graphically with the ability to "drill down" into the data of interest.

Network Management Tasks that would be included as supporting this function include: